

## Section 2. General Requirements

**1-200. General.** Contractors shall **protect** all classified information to which they have access or custody. A contractor performing work within the confines of a Federal installation shall safeguard classified information in accordance with provisions of this Manual and/or with the procedures of the host installation or agency.

**1-201. Facility Security Officer (FSO).** The contractor shall appoint a U.S. citizen employee, who is cleared as part of the facility clearance (FCL), to be the FSO. The FSO will supervise and direct security measures necessary for implementing this Manual and related Federal requirements for classified information. The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.

1-202. Standard **Practice Procedures.** The contractor shall implement all terms of this Manual applicable to each of its cleared facilities. Written procedures shall be prepared when the FSO believes them to be necessary for effective implementation of this Manual or when the cognizant security office (CSO) determines them to be necessary to reasonably foreclose the possibility of loss or compromise of **classified information**.

**1-203. One-Person Facilities.** A facility at which only one person is assigned shall establish procedures for CSA notification after death or incapacitation of that person. The current combination of the facility's security container shall be provided to the CSA, or in the case of a multiple facility organization, to the home office.

1-204. Cooperation with **Federal Agencies.** Contractors shall cooperate with Federal agencies during official inspections, investigations concerning the protection of classified information, and during the conduct of personnel security investigations of present or former employees and others. This includes providing suitable arrangements with the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review, when requested, and rendering other necessary assistance.

**1-205. Agreements with Foreign Interests.** Contractors shall establish procedures to ensure compliance with governing export control laws before executing any agreement with a foreign interest that involves access to

U.S. classified information by a foreign national. Contractors must also comply with the foreign ownership, control or influence requirements in this Manual. Prior to the execution of such agreements, review and approval are required by the State Department and release of the classified information must be approved by the U.S. Government. Failure to comply with Federal licensing requirements may render a contractor ineligible for a facility clearance.

1-206. **Security Training and Briefings.** Contractors are responsible for advising all cleared employees, including those outside the United States, of their individual responsibility for safeguarding classified information. In this regard, contractors shall provide security training as appropriate, and in accordance with Chapter 3, to cleared employees by initial briefings, refresher briefings, and debriefings.

1-207. **Security Reviews.**

a. **Government Reviews.** Aperiodic security reviews of **all** cleared contractor facilities **will** be conducted to ensure that safeguards employed by contractors are adequate for the protection of classified information.

(1) **Review Cycle.** The CSA will determine the frequency of security reviews, which may be increased or decreased for sufficient reason, consistent with risk management principals. Security reviews may be conducted no more often than once every 12 months unless special circumstances exist.

(2) **Procedures.** Contractors will normally be provided notice of a forthcoming review. Unannounced reviews may be conducted at the discretion of the CSA. Security reviews necessarily subject **all** contractor employees and **all** areas and receptacles under the control of the contractor to examination. However, every effort will be made to avoid unnecessary intrusion into the personal effects of contractor personnel. The physical examination **of the** interior space of equipment not authorized to secure classified material will always be accomplished in the presence of **a** representative of the contractor.

- (3) Reciprocity. Each CSA is responsible for ensuring that redundant and duplicative security review, and audit activity of its contractors is held to a minimum, including such activity conducted at common facilities by other CSA's. Appropriate intra and/or inter-agency agreements shall be executed to fulfill this cost-sensitive imperative. Instances of redundant and duplicative security review and audit activity shall be reported to the Director, Information Security Oversight Office (ISOO) for resolution.

**b. Contractor Reviews.** Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principals.

**1-208. Hotlines.** Federal agencies maintain hotlines to provide an “unconstrained avenue for government and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotlines may be used, if necessary, for reporting matters of national security significance. CSA hotline addresses and telephone numbers are as follows:

**Defense Hotline**  
**The Pentagon**  
**Washington, DC 20301-1900**  
**(800) 424-9098**  
**(703) 693-5080**

**NRC Hotline**  
**U.S. Nuclear Regulatory Commission**  
**Office of the Inspector General**  
**Mail Stop TSD 28**  
**Washington, D.C. 20555-0001**  
**(800) 233-3497**

**CIA Hotline**  
**Office of the Inspector General**  
**Central Intelligence Agency**  
**Washington, D.C. 20505**  
**(703) 874-2600**

**DOE Hotline**  
**Department of Energy**  
**Office of the Inspector General**  
**1000 Independence Avenue, S.W.**  
**Room 5A235**  
**Washington, D.C. 20585**  
**(202) 586-4073**  
**(800) 541-1625**

**1-209. Classified Information Procedures Act (CIPA).** (P.L. 96-456, 94 STAT. 2025) The provisions of this Manual do not apply to proceedings in criminal cases involving classified information, and appeals therefrom, before the United States District Courts, the Courts of Appeal, and the Supreme Court. Contractors and their employees are not authorized to afford defendants, or persons acting for the defendant, regardless of their personnel security clearance status, access to classified information except as otherwise authorized by a protective order issued pursuant to the CIPA.